

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

United States of America
v.
Curtis Oglesby, Jr. (XX/XX/1998)

Case No. 25-801M(NJ)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of October 2023 - May 2024 in the county of Milwaukee in the
Eastern District of Wisconsin, the defendant(s) violated:

Code Section

18 U.S.C. §§ 656; 1957

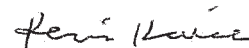
Offense Description

Embezzlement by bank agent; money laundering

This criminal complaint is based on these facts:

See Attached Affidavit.

☒ Continued on the attached sheet.



Complainant's signature

Kevin Kaiser, FBI SA

Printed name and title

Sworn via telephone; transmitted via email
pursuant to Fed. R. Crim. 4.1

Date: 2/3/2025

City and state: Milwaukee, WI



Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANT AND COMPLAINT**

I, Kevin Kaiser, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AFFIANT'S BACKGROUND

1. Your affiant makes this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the following premises, vehicle, and person, device further described in Attachments A1, Attachments A2, and Attachments A3 (collectively, "Attachments A"), for the things described in Attachment B:

A1. 3140 West Howard Avenue, Apt #9, Greenfield, Wisconsin ("SUBJECT PREMISES");

A2. A 2020 black Jeep Grand Cherokee bearing Wisconsin license plate AXT-1387 and VIN #1C4RJFDJ6LC413456 ("SUBJECT VEHICLE");

A3. The person of CURTIS OGLESBY JR (DOB: XX/XX/1998) ("SUBJECT PERSON" or "OGLESBY JR").

2. Your affiant further submits this affidavit in support of a criminal complaint and arrest warrant naming OGLESBY JR.

3. Your affiant is a Special Agent with the Federal Bureau of Investigation (FBI) and have been since April 2023. Since April 2023, Affiant has been assigned to the FBI Milwaukee Area Violent Crimes Task Force, a multi-jurisdictional law enforcement entity charged with investigating violations of federal law, including bank robberies, commercial robberies, armed motor vehicle robberies, and other violent crime matters, as defined under Title 18 of the United States Code. Affiant has been trained in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, and probable

cause. Affiant has participated in criminal investigations, surveillance, search warrants, interviews, and debriefs of arrested subjects. As a result of this training and investigative experience, affiant has learned how and why thieves and robbers typically conduct various aspects of their criminal activities. Affiant has experience in the investigation, apprehension and prosecution of individuals involved in federal criminal offenses, the use of cellular devices to commit those offenses and the available technology that can be used by law enforcement to assist in identifying the users of cellular devices and their location.

4. Affiant has participated in numerous investigations involving the seizure of cellular phones and other digital storage devices, and the subsequent analysis of electronic data stored within these devices. This has led to evidence of the crimes under investigation and corroborated information already known or suspected by law enforcement. Affiant has regularly used electronic evidence to find proof relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of suspects and conspirators.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

6. Affiant makes this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the search of (i) the premises located 3140 West Howard Avenue, Apartment 9, Greenfield, Wisconsin, further described in Attachment A1 ("SUBJECT PREMISES"), (ii) a 2020 Jeep Grand Cherokee bearing Wisconsin license plate AXT-1387 and VIN #1C4RJFDJ6LC413456 described in Attachment A2 ("SUBJECT VEHICLE"), and (iii) the person of OGLESBY JR described in Attachment A3

(“SUBJECT PERSON”) for the purpose of locating any evidence of the crime and searching any cellular device found in SUBJECT PREMISES, in the SUBJECT VEHICLE, or on the SUBJECT PERSON.

7. Based on the facts as set forth in this affidavit, there is probable cause to believe that violations of theft or embezzlement by a bank agent, in violation of Title 18, United States Code, Section 656, and money laundering, in violation of Title 18, United States Code, Section 1957, (collectively, the “TARGET OFFENSES”) have been committed by OGLESBY JR. There is also probable cause to search the SUBJECT PREMISES and SUBJECT VEHICLE (including each cellular phone or storage medium found therein) for evidence of these crimes, as further described in Attachment B. Furthermore, there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of the are present in the SUBJECT PREMISES, in the SUBJECT VEHICLE and on the SUBJECT PERSON.

8. Pursuant to my official duties, affiant is submitting this Affidavit in support of an application for a criminal complaint and a search warrants, relating to violations of federal law, including violations of Title 18, United States Code, Section 656, and Title 18, United States Code, Section 1957.

PURPOSE OF AFFIDAVIT

A. Individual for Whom a Criminal Complaint is Sought

9. This affidavit is being submitted in support of both applications for a search warrant and a criminal complaint naming the following individual:

- CURTIS OGLESBY JR / Date of Birth (03/26/1998)

B. Property for Which Search Warrant is Sought

10. The SUBJECT PREMISES, 3140 West Howard Avenue, Apartment 9, Greenfield, Wisconsin, is a Southgate apartment complex to include 15 apartments with entry doors on the north and south ends of the building. The numerals 3140 are displayed on the south end of the building. A picture of the location follows below. According to Wisconsin Department of Transportation, OGLESBY JR's address is listed as 3140 West Howard Avenue, Apartment 9, Greenfield, Wisconsin. According to commercial databases, JESSICA SORENSEN, DOB (XX/XX/1995) ("SORENSEN"), a listed associate of OGLESBY JR, also resides at this address. Over the course of this investigation, agents have observed OGLESBY JR at this location multiple times, as well as his 2020 Jeep Grand Cherokee bearing WI Registration AXT-1387. Affiant knows OGLESBY JR is currently receiving mail at the 3140 West Howard Avenue, Apartment 9, address. Affiant is aware the mailbox for Apartment 9 has the names OGLESBY and SORENSEN on it.



PROBABLE CAUSE

11. The Brink's Company ("Brinks") is a provider of cash and valuables management services, and of ATM management services. Their clients include financial institutions and other commercial operations. OGLESBY JR was employed by Brinks as an armed messenger from October 30, 2023, through May 3, 2024. Representatives from Brinks Regional Security provided your affiant with supporting documentation relating to 44 cash shortages identified between December 21, 2023, and April 8, 2024. The shortages represent a combination of funds missing from bank ATM machines and funds missing from secured boxes ("Brinks boxes") set up at various vendor locations. Brinks boxes are used to store cash tendered to vendors who accept cash as payment for their goods and services. The vendors contract with Brinks for the removal, transport, and subsequent deposit of the cash.

12. As more fully described below, Brinks' records show that, from between approximately October 2023 and May 2024, OGLESBY JR embezzled approximately \$434,618.55 from Brinks by taking money from bank ATMs and Brinks boxes during his employment as an armed Brinks messenger. As a Brinks messenger, OGLESBY JR was responsible for transporting cash by armored vehicle to and from federally insured financial institution ATMs, as well as Brinks boxes. Bank tellers reported cash shortages when they balanced the residual amounts on certain ATMs associated with OGLESBY JR. Brinks personnel also determined deposit bags were missing from the Brinks boxes serviced by OGLESBY JR. An investigation by Brinks identified OGLESBY JR as the messenger servicing the locations which incurred these shortages. Records affiant has reviewed similarly demonstrate that OGLESBY JR proceeded to spend the stolen monies on personal items, such as jewelry, gun(s), and a vehicle.

OGLESBY JR also deposited approximately \$48,795.00 in cash into his JP Morgan Chase Bank checking account during this time.

13. The documentation supplied by Brinks showed that shortages were reported after the servicing of 15 ATM machines and from 29 bags deposited into Brinks boxes, between December 21, 2023, and April 8, 2024. Each of the locations were serviced by OGLESBY JR. during the time periods when the shortages occurred.

14. In the cases involving the Brinks boxes, Brinks' documents reflect that OGLESBY JR was the only person with access to the boxes when the shortages were reported (with one exception). Brinks security personnel informed affiant that for each deposit made by a vendor into a Brinks box, the vendor making the deposit scanned a bar code which was attached to the bag holding the vendor's cash deposit. The scanned bar code alerted Brinks that a deposit had been made and was available for pickup. In many instances, multiple bags were deposited during a period of time which might span several days, before a Brinks messenger was dispatched to retrieve the cash bags deposited into the Brinks box. Brinks' operating procedures stipulate that when a Brinks messenger retrieves the bags containing the cash, the messenger is required to scan the bar code attached to the bag in order to register the bag in Brinks' security system. Brinks security personnel informed me that their records indicate OGLESBY JR did not scan pre-registered deposit bags on numerous occasions. In many instances, multiple deposit bags were stolen during the same messenger pickup assignment by OGLESBY JR.

15. In the cases involving missing funds from ATM machines, Brinks' security personnel determined that OGLESBY JR was the assigned Brinks messenger either when the ATM machine was replenished, or when residual cash was retrieved from the ATM machine.

16. A review of OGLESBY JR's JP Morgan Chase Bank checking account was reflective of him possessing an uncharacteristic amount of cash during the period of time that he was employed with Brinks. To be specific, these records show that OGLESBY JR made cash deposits of \$1,000.00 or more during a single day on 12 dates between January 8, 2024, and April 15, 2024, including cash deposits of \$5,000.00 on March 25, 2024; \$9,900.00 on March 28, 2024; and, \$10,000.00 on April 15, 2024. During the 10 months preceding OGLESBY JR's employment with Brinks, he made two cash deposits of \$1,000.00 or more (\$1,000.00 and \$1,500.00). During the six-month time period after OGLESBY JR was terminated by Brinks, he did not make any cash deposits of \$1,000.00 or more.

17. The documentation furnished by Brinks determined the following thefts from ATM machines occurred between March 11, 2024, and March 28, 2024:

<u>Date Range</u>	<u>Amount Stolen</u>	<u>Date Serviced by OGLESBY JR</u>
3/11/2024-3/19/2024	\$ 60,180.00	3/19/2024
3/12/2024-3/15/2024	\$ 49,720.00	3/12/2024
3/19/2024-3/22/2024	\$ 59,800.00	3/19/2024
3/21/2024-3/28/2024	\$ 41,200.00	3/21/2024

18. On March 21, 2024, OGLESBY JR purchased four jewelry items from Pak's Jewelers for \$60,000.00. The jewelry items were described as a diamond Cuban link necklace, a diamond cluster link 8" bracelet, a diamond cluster link 24.5" necklace, and a custom gold and diamond teeth covering. The IRS Form 8300 completed as a result of the purchase indicated that all of the bills tendered by OGLESBY JR were \$100 bills (which is the predominant bill denomination used by the institutions OGLESBY JR serviced during his time at Brinks). On April 5, 2024, OGLESBY JR purchased two jewelry items for \$34,000.00 on layaway with a cash down

payment of \$5,100.00, and an additional payment of \$10,000.00 on April 9, 2024. The two jewelry items were described as a diamond Cuban link 8” bracelet and a diamond Cuban link 24” necklace. The IRS Form 8300 once again identified all of the bills tendered by OGLESBY JR as \$100 bills.

19. On April 6, 2024, OGLESBY JR made a \$40,000.00 cash down payment on a 2020 Jeep Grand Cherokee. Here again, the IRS Form 8300 completed as a result of the purchase stated that all of the bills tendered were \$100 bills.

20. The \$48,795.00 in cash deposited into OGLESBY JR’s JP Morgan Chase Bank checking account between December 2023 and May 2024, was in addition to OGLESBY JR’s earnings from Brinks, which were deposited via direct deposit.

21. On January 21, 2025, Brinks Milwaukee Trainer D.H. stated in the last few months of OGLESBY JR’s employment, OGLESBY JR directly told D.H. that he was gifted a new Jeep paid for by his mother and sister for his birthday. OGLESBY JR also stated several times that he went to a gun store to purchase new firearms around the same time.

22. On June 18, 2024, Brinks Regional Security Manager M.N. spoke to OGLESBY JR regarding the cash variances over the telephone. According to M.N., OGLESBY JR indicated he was responsible for the variances, by stating that he needed the money to pay for medical bills and that there were no funds left. However, OGLESBY JR indicated he was still in possession of the Jeep Grand Cherokee he stated his sister purchased for him.

23. On January 27, 2025, Brinks Regional Security Manager M.N. and Branch Manager A.S. advised that the Brinks Milwaukee branch that OGLESBY JR was employed through did not experience this pattern of shortages prior to OGLESBY JR’s employment and that this pattern of shortages ceased after OGLESBY JR’s termination.

24. A review of OGLESBY JR's checking account at JP Morgan Chase Bank, the same account into which his payroll checks from Brinks were direct-deposited, determined that the balance in the account during the 90 days preceding the purchase of the jewelry items and the Jeep Grand Cherokee referenced above was never higher than \$15,055.34, establishing that the account did not serve as the origin for the cash payments totaling \$115,100.00. Your affiant submits there is probable cause to believe that the \$115,100.00 used to pay for the above-mentioned jewelry and Jeep funds stolen by OGLESBY JR from Brinks, such that those payments amount to violations of 18 U.S.C. § 1957.

TECHNICAL TERMS

25. Based on my training and experience, affiant uses the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading

information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved

in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

26. Based on my knowledge, training, and experience, as well as my conversations with other Special Agents of the Federal Bureau of Investigation, who are experienced with electronic communication systems, affiant knows that the electronic Devices described above have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. Based on affiant's knowledge, training, and experience, as well as my conversations with other Special Agents of the Federal Bureau of Investigation who are experienced with electronic communication systems, affiant knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of use, who used it, and when.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant affiant is applying for would permit the examination of the device consistent with the warrant. The examination may require authorities, including state of Wisconsin

law enforcement officers, to employ techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

ANY CELL PHONE OR ELECTRONIC DEVICE IS LIKELY TO CONTAIN
INFORMATION RELEVANT TO THIS INVESTIGATION

30. Based upon my experience and training, consultation with other law enforcement officers experienced in theft or embezzlement by a bank agent conspiracies and investigations, and all the facts and opinions set forth in this affidavit, affiant knows that individuals involved in theft or embezzlement by a bank agent often utilize cell phones or other electronic media that contain:

- a. Communications, photographs, videos, or other data regarding the thefts/embezzlement, along with any proceeds derived from the thefts/embezzlement;
- b. Communications, photographs, videos, or other data shared with co-conspirators coordinating and then executing the thefts/embezzlement, to include coordinating and executing flight from the thefts/embezzlement;
- c. Celebratory remarks after the successful completion of the thefts/embezzlement;
- d. Internet and Web-search history relating to the thefts/embezzlement;
- e. Proceeds or otherwise attempting to sell, spend, hide, or give away what appears to be proceeds from the thefts/embezzlement; and
- f. Communications, photographs, videos, or other data relevant to covering up or hiding their crimes and escaping or hiding from law enforcement.
- g. Subscriber Identity Module (SIM) Cards also known as subscriber identity modules are smart cards that store data for GSM cellular telephone subscribers. Such data

includes user identity, location and phone number, network authorization data, personal security keys, contact lists and stored text messages. Much of the evidence generated by a use of a cellular telephone would likely be stored on any SIM Card that has been utilized in connection with that telephone. Based upon my experience investigating theft or embezzlement by a bank agent and the investigation in this case, affiant believes that any cell phone or electronic media recovered from OGLESBY JR may have been used after the fact to conceal, advance, and/or profit from the theft events in this case. In addition, affiant knows data may be transferred from one cellular telephone to another. Therefore, affiant knows that recent calls made and received, telephone numbers, contact names, electronic mail (e-mail) addresses, appointment dates, text messages, pictures and other digital information are stored in the memory of any cell phone or electronic media recovered from OGLESBY JR may identify the persons involved in in the thefts, including OGLESBY JR himself. Accordingly, based upon my experience and training, consultation with other law enforcement officers experienced in theft or embezzlement by a bank agent investigations, and all the facts and opinions set forth in this affidavit, affiant believes that information relevant to theft/embezzlement activities, such as telephone numbers, made and received calls, contact names, electronic mail (e-mail) addresses, appointment dates, messages, pictures and other digital information are likely to be stored in the memory of any cell phone or electronic media recovered from OGLESBY JR.

- h. Finally, affiant also knows that theft or embezzlement by bank agent conspiracies entail intricate planning to successfully initiate, execute, and then evade detection

by law enforcement. In my professional experience, this requires planning and coordination in the weeks and often months prior to the event and also requires communication in the weeks and months following the event. Considering that data may be transferred from one cell phone to another, affiant respectfully requests permission to search any cell phone or electronic media recovered from OGLESBY JR for items listed in Attachment B.

OTHER ISSUES

31. Affiant knows, based upon training and experience, that evidence of theft or embezzlement can be secreted in any part of a residence including garages, storage areas related to the premises, vehicles on and associated with the premises, and on persons engaged in theft or embezzlement within the residence; that through personal training and experience in investigating thefts/embezzlement, affiant knows that the execution of a search warrant usually results in the seizure of such items of personal property as utility bills, canceled mail envelopes, bank statements, keys, photographs, videotapes, and other items or documents which establish the identities of persons residing in or having control of the premise; and that these items can be stored in various locations accessible to the target residence including vehicles and garages. Therefore, affiant believes it is reasonable to believe that an individual engaged in thefts/embezzlement would conceal evidence related to thefts or embezzlement in multiple areas associated with their residence including vehicles, garages, storage areas, and basements, and include such locations in the definition of the **TARGET PREMISES**.

32. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **TARGET PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive,

cellular telephone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

33. *Probable cause.* Affiant submits that if a computer, cellular telephone, or storage medium is found on the **TARGET PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on affiant's knowledge, training, and experience, affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

34. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **TARGET PREMISES** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the

chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to operate a website that is used for illegal conduct, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, affiant believes that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

35. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware

and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off- site reviewing with specialized forensic tools.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant affiant is applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

37. The warrant affiant is applying for would permit law enforcement to obtain from the display of physical biometric characteristics (such as fingerprint, thumbprint, facial, or iris characteristics) to unlock devices subject to search and seizure pursuant to this warrant. Affiant seek this authority based on the following:

38. Affiant knows from training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices, and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices

offer a combination of these biometric features, and the user of such devices can select which features they would like to use.

39. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

40. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes, and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

41. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device through his or her irises. For example, Samsung offers an Iris Scanner, which uses the biometric information of an individuals’ irises to identify the user.

42. Affiant knows from training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect

a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

43. As discussed in this affidavit, based on my training and experience affiant believes that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

44. Affiant knows from training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered within a certain period of time. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

45. Due to the foregoing, with respect to any person who is located in the **TARGET PREMISES** during the execution of the search and who is reasonably believe by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of this warrant, it is requested that law enforcement personnel may (1) press or swipe the fingers (including thumbs) of the person to the fingerprint scanner of the device found at the premises; or (2) hold the device

in front of the person's face to activate the facial and/or iris recognition features, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

46. Because at least two people share the **TARGET PREMISES** as a residence, it is possible that the **TARGET PREMISES** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

REQUEST FOR SEIZURE

47. *VEHICLE* - On October 9, 2024, and November 19, 2024, affiant surveilled OGLESBY JR's known address of 3140 West Howard Avenue, Apartment 9, Greenfield, Wisconsin. Affiant observed a 2020 Jeep Grand Cherokee bearing Wisconsin license plate AXT-1387 parked in the parking lot of the apartment complex. The Wisconsin Department of Transportation identified OGLESBY JR as the registered owner of this Jeep Grand Cherokee. Affiant requests car keys/key fob to be seized with the Grand Cherokee. Affiant also obtained the below photograph during the course of this investigation:



48. *JEWELRY* - The jewelry items are described as:

- a. A 26" diamond Cuban link necklace
- b. An 8" diamond cluster link bracelet
- c. A 24.5" diamond cluster link necklace
- d. A custom gold and diamond teeth covering
- e. An 8" diamond Cuban link bracelet
- f. A 24" diamond Cuban link necklace





d.



e.



f.

CONCLUSION

49. Your affiant believes there are, located within the premises and vehicles described in Attachments A-1 and A-2, materials, documents and records, to include cellular devices, electronic devices, cash, and jewelry items, that reflect CURTIS OGLESBY JR's involvement in theft or embezzlement by bank agent and money laundering.

50. For all of the foregoing reasons, affiant requests authorization to search the premises, vehicle, and person more fully described in Attachments A for the things described in Attachment B.

ATTACHMENT A1

Property to Be Searched

The property to be searched is 3140 West Howard Avenue, Apartment #9, Greenfield, Wisconsin, part of the Southgate Apartments further described as the FIRST-floor unit located on the west side of the building depicted below (“TARGET PREMISES”). The building consists of dark brown siding with brown trim. The numbers “3140” are affixed to the exterior of the south end of the building.



ATTACHMENT A2

MATTER NO. 2020R00324

Property to Be Searched

The property to be searched is a black 2020 Jeep Grand Cherokee bearing Wisconsin license plate AXT1387 and VIN 1C4RJFDJ6CL413456 (“TARGET VEHICLE”).



ATTACHMENT A3

MATTER NO. 2020R00324

Person to Be Searched

The person to be searched is CURTIS OGLESBY JR (DOB: XX/XX/1998) (“SUBJECT PERSON” or “OGLESBY JR”).

ATTACHMENT B

MATTER NO. 2020R00324

Property to be seized

1. All records, information, and items relating to violations of Title 18, United States Code, Section 656, and Title 18, United States Code, Section 1957, those violations involving CURTIS OGLESBY JR and occurring between October 2023 and May 2024, including:

- a. Evidence of the crimes described above;
- b. Preparatory steps taken in furtherance of those crimes;
- c. Evidence of motive, intent, or knowledge of the crimes described above;
- d. Evidence indicating how and when electronic devices were accessed or used, to determine the chronological and geographic context of access, use, and events relating to the crimes under investigation;
- e. Jewelry purchased by CURTIS OGLESBY JR from Paks Jewelers;
- f. Guns purchased from January 2024 - Present;
- g. CURTIS OGLESBY JR'S cellular device(s);
- h. A 2020 black Jeep Grand Cherokee bearing Wisconsin license plate AXT-1387 and VIN# 1C4RJFDJ6LC413456, to include car keys/key fob;
- i. Cash;
- j. Documentation from October 30, 2023, to present which is indicative of financial accounts held by OGLESBY JR and/or SORENSEN; assets purchased by OGLESBY JR and/or SORENSEN; evidence of cryptocurrency transactions; evidence of real estate and/or vehicle purchases; evidence of electronics and/or luxury clothing purchases; and, evidence of jewelry purchases;
- k. Any money straps, money bags, and any other property containing a "Brinks" logo, and/or items resembling those used by Brinks.